Extractors for Jacobian of hyperelliptic curves of genus 2 in odd characteristic

Extractors for Jacobian of Hyperelliptic Curves of Genus 2 in Odd Characteristic

Reza Rezaeian Farashahi[1,2]

[1] Dept. of Mathematics and Computer Science, TU Eindhoven,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
[2] Dept. of Mathematical Sciences, Isfahan University of Technology,
P.O. Box 85145 Isfahan, Iran

Abstract. We propose two simple and efficient deterministic extractors for $J(\mathbb{F}_q)$, the Jacobian of a genus 2 hyperelliptic curve H defined over $\mathbb{F}_q$, for some odd q. Our first extractor, `SEJ`, called *sum extractor*, for a given point D on $J(\mathbb{F}_q)$, outputs the sum of abscissas of rational points on H in the support of D, considering D as a reduced divisor. Similarly the second extractor, `PEJ`, called *product extractor*, for a given point D on the $J(\mathbb{F}_q)$, outputs the product of abscissas of rational points in the support of D. Provided that the point D is chosen uniformly at random in $J(\mathbb{F}_q)$, the element extracted from the point D is indistinguishable from a uniformly random variable in $\mathbb{F}_q$. Thanks to the Kummer surface $\mathcal{K}$, that is associated to the Jacobian of H over $\mathbb{F}_q$, we propose the *sum* and *product* extractors, `SEK` and `PEK`, for $\mathcal{K}(\mathbb{F}_q)$. These extractors are the modified versions of the extractors `SEJ` and `PEJ`. Provided a point K is chosen uniformly at random in $\mathcal{K}$, the element extracted from the point K is statistically close to a uniformly random variable in $\mathbb{F}_q$.

Keywords: Jacobian, Hyperelliptic curve, Kummer surface, Deterministic extractor.

1 Introduction

A deterministic extractor for a set S is a function that converts a random point on S to a bit-string of fixed length that is statistically close to uniformly random. In this paper, we propose two simple and efficient deterministic extractors for $J(\mathbb{F}_q)$, the Jacobian of a hyperelliptic curve H of genus 2 defined over $\mathbb{F}_q$, for some odd q. Our first extractor, `SEJ`, called *sum extractor*, for a given point D on $J(\mathbb{F}_q)$, outputs the sum of abscissas of rational points on H in the support of D, considering D as a reduced divisor. Similarly the second extractor, `PEJ`, called *product extractor*, for a given point D on the $J(\mathbb{F}_q)$, outputs the product of abscissas of rational points in the support of D. Provided that the point D is chosen uniformly at random in $J(\mathbb{F}_q)$, the element extracted from the point D is indistinguishable from a uniformly random variable in $\mathbb{F}_q$.

Let $\mathcal{K}$ be the Kummer surface associated to the Jacobian of H over $\mathbb{F}_q$. Then there is a map κ from $J(\mathbb{F}_q)$ to $\mathcal{K}(\mathbb{F}_q)$, so that a point and it's opposite in $J(\mathbb{F}_q)$ are mapped to the same value. Using this map, we propose two simple

S.D. Galbraith (Eds.): Cryptography and Coding 2007, LNCS 4887, pp. 313–335, 2007.

and efficient deterministic extractors, SEK and PEK, for the Kummer surface $\mathcal{K}$. If a point K is chosen uniformly at random in $\mathcal{K}$, the element extracted from the point K is statistically close to a uniformly random variable in $\mathbb{F}_q$.

The use of hyperelliptic curves in public key cryptography was first introduced by Koblitz in [15]. The security of hyperelliptic cryptosystems is based on the difficulty of discrete logarithm problem in the Jacobian of these curves. Hyperelliptic curves of genus 2 are undergoing intensive study. They were shown to be competitive with elliptic curves in speed and security. Various researchers have been optimizing genus 2 arithmetic (see [2,16,17]). The security of genus 2 hyperelliptic curves is assumed to be similar to that of elliptic curves of the same group size (e.g see [10]).

The use of Kummer surface associated to the Jacobian of a genus 2 curve is proposed for faster arithmetic (see [7,11,16]). The scalar multiplication on the Jacobian can be used to define a scalar multiplication on the Kummer surface. It could be used to construct a Diffie-Hellman protocol (see [21]). In addition, it is shown in [21], solving the discrete logarithm problem on the Jacobian is polynomial time equivalent to solving the discrete logarithm problem on the kummer surface.

The problem of converting random points of a variety (e.g a curve or Jacobian of a curve) into random bits has several cryptographic applications. Such applications are key derivation functions, key exchange protocols and design of cryptographically secure pseudorandom number generators. As examples we can mention the well-known Elliptic Curve Diffie-Hellman protocol and Diffie-Hellman protocol in genus 2. By the end of Diffie-Hellman protocol, the parties agree on a common secret element of the group, which is indistinguishable from a uniformly random element under the decisional Diffie-Hellman assumption (denoted by DDH). However the binary representation of the common secret element is *distinguishable* from a uniformly random bit-string of the same length. Hence one has to convert this group element into a random-looking bit-string. This can be done using a deterministic extractor.

At the moment, several deterministic randomness extractors for elliptic curves are known. Kaliski [14] shows that if a point is taken uniformly at random from the union of an elliptic curve and its quadratic twist then the abscissa of this point is uniformly distributed in the finite field. Then Chevassut et al. [5], proposed the TAU technique. This technique allows to extract almost all the bits of the abscissa of a point of the union of an elliptic curve and its quadratic twist. Gürel [12] proposed an extractor for an elliptic curve defined over a quadratic extension of a prime field. It extracts almost half of the bits of the abscissa of a point on the curve. Then, Farashahi and Pellikaan proposed the similar extractor, yet more general, for hyperelliptic curves defined over a quadratic extension of a finite filed in odd characteristic [8]. Furthermore, their result for elliptic curves improves the result of [12]. Two deterministic extractors for a family of binary elliptic curves are proposed by Farashahi et al. [9]. It is shown that half of the bits of the abscissa of a point on the curve can be extracted. They also proposed two deterministic extractors for the main subgroup of an ordinary elliptic curve

that has minimal 2-torsion. In our knowledge, up to now, no extractor is defined for the Jacobian of a hyperelliptic curve.

We organize the paper as follows. In the next section we introduce some notations and recall some basic definitions. In Section 3, we propose extractors SEJ and PEJ for $J(\mathbb{F}_q)$, the Jacobian of a genus 2 hyperelliptic curve H over $\mathbb{F}_q$. We show that the outputs of these extractors, for a given uniformly random point of $J(\mathbb{F}_q)$, are statistically close to a uniformly random variable in $\mathbb{F}_q$. For the analysis of these extractors, we need some bounds on the cardinalities of $\mathtt{SEJ}^{-1}(a)$ and $\mathtt{PEJ}^{-1}(b)$, for all $a, b \in \mathbb{F}_q$. We give our estimates for them in Theorems 2 and 3. Then, in Section 4, we give the proofs of the main Theorems 2 and 3. In Section 5, we propose two extractors SEK and PEK for $\mathcal{K}(\mathbb{F}_q)$, the Kummer surface related to $J(\mathbb{F}_q)$. These extractors are modified versions of the previous extractors, using the map κ from $J(\mathbb{F}_q)$ to $\mathcal{K}(\mathbb{F}_q)$. We conclude our result in Section 6. Furthermore, in appendix, we introduce some corresponding problems for the proof of the main Theorem 2.

2 Preliminaries

Let us define the notations and recall the basic definitions that are used throughout the paper.

Notation. Denote by $\mathbb{Z}_n$ the set of nonnegative integers less than n. A field is denoted by $\mathbb{F}$ and its algebraic closure by $\overline{\mathbb{F}}$. Denote by $\mathbb{F}^*$ the set of nonzero elements of $\mathbb{F}$. The finite field with q elements is denoted by $\mathbb{F}_q$, and its algebraic closure by $\overline{\mathbb{F}}_q$. Let C be a curve defined over $\mathbb{F}_q$, then the set of $\mathbb{F}_q$-rational points on C is denoted by $C(\mathbb{F}_q)$. The x-coordinate of a point P on a curve is denoted by x_P. The cardinality of a finite set S is denoted by $\#S$. We make a distinction between a variable $\mathbf{x}$ and a specific value x in $\mathbb{F}$.

2.1 Finite Field Notation

Consider the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, where $q = p^k$, for some odd prime number p and positive integer k. Fix a polynomial representation $\mathbb{F}_{q^2} \cong \mathbb{F}_q[t]/(t^2 - \alpha)$, where α is not a quadratic residue in $\mathbb{F}_q$. Then $\mathbb{F}_{q^2}$ is a vector space over $\mathbb{F}_q$ which is generated by the basis $\{1, t\}$. That means every element x in $\mathbb{F}_{q^2}$ can be represented in the form $x = x_0 + x_1 t$, where x_0 and x_1 are in $\mathbb{F}_q$.

Let $\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$ be the Frobenius map defined by $\phi(x) = x^q$.

2.2 Hyperelliptic Curves

Definition 1. *An absolutely irreducible nonsingular curve $\mathcal{H}$ of genus at least* 2 *is called* hyperelliptic *if there exists a morphism of degree* 2 *from $\mathcal{H}$ to the projective line.*

Theorem 1. *Let $\mathcal{H}$ be a hyperelliptic curve of genus g over $\mathbb{F}_q$, where q is odd. Then $\mathcal{H}$ has a plane model of the form*

$$\mathbf{y}^2 = f(\mathbf{x}),$$

where f is a square-free polynomial and $2g+1 \leq \deg(f) \leq 2g+2$. The plane model is singular at infinity. If $\deg(f) = 2g+1$ then the point at infinity ramifies and $\mathcal{H}$ has only one point at infinity. If $\deg(f) = 2g+2$ then $\mathcal{H}$ has zero or two $\mathbb{F}_q$-rational points at infinity.

Proof. See [1,6]. □

In this paper we consider a hyperelliptic curve $\mathcal{H}$ that has only one point at infinity. One calls $\mathcal{H}$ an *imaginary* hyperelliptic curve.

2.3 Jacobian of a Hyperelliptic Curve

Let $\mathcal{H}$ be an imaginary hyperelliptic curve of genus g over $\mathbb{F}_q$, where q is odd. Then $\mathcal{H}$ has a plane model of the form $\mathbf{y}^2 = f(\mathbf{x})$, where f is a square-free polynomial and $\deg(f) = 2g+1$. For any subfield $\mathbb{K}$ of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$, the set

$$\mathcal{H}(\mathbb{K}) = \{(x,y) : x,y \in \mathbb{K},\ y^2 = f(x)\} \cup \{P_\infty\},$$

is called the set of $\mathbb{K}$-*rational points* on $\mathcal{H}$. The point P_∞ is called the *point at infinity* for $\mathcal{H}$. A point P on $\mathcal{H}$, also written $P \in \mathcal{H}$, is a point $P \in \mathcal{H}(\overline{\mathbb{F}}_q)$. The negative of a point $P = (x,y)$ on $\mathcal{H}$ is defined as $-P = (x,-y)$ and $-P_\infty = P_\infty$.

Definition 2. *A* divisor *D on $\mathcal{H}$ is a formal sum of points on $\mathcal{H}$*

$$D = \sum_{P \in \mathcal{H}} m_P P,$$

where $m_P \in \mathbb{Z}$, and only a finite number of the m_P are nonzero. The degree *of D is defined by $\deg D = \sum_{P \in \mathcal{H}} m_P P$. The divisor D is said to be* defined over $\mathbb{K}$*, if for all automorphisms φ in the Galois group of $\mathbb{K}$, $\varphi(D) = \sum_{P \in \mathcal{H}} m_P\, \varphi(P) = D$, where $\varphi(P) = (\varphi(x), \varphi(y))$ if $P = (x,y)$ and $\varphi(P_\infty) = P_\infty$.*

The set of all divisors on $\mathcal{H}$ defined over $\mathbb{K}$, denoted by $Div_{\mathcal{H}}(\mathbb{K})$, forms an additive abelian group under the addition rule

$$\sum_{P \in \mathcal{H}} m_P P + \sum_{P \in \mathcal{H}} n_P P = \sum_{P \in \mathcal{H}} (m_P + n_P) P.$$

The set $Div^0_{\mathcal{H}}(\mathbb{K})$ of all divisors on $\mathcal{H}$ of degree zero defined over $\mathbb{K}$ is a subgroup of $Div_{\mathcal{H}}(\mathbb{K})$. In particular, $Div^0_{\mathcal{H}} = Div^0_{\mathcal{H}}(\overline{\mathbb{K}})$.

Let $\mathbb{K}[\mathcal{H}]$ be the *coordinate ring* of the plain model of $\mathcal{H}$ over $\mathbb{K}$. Then the *function field* of $\mathcal{H}$ over $\mathbb{K}$ is the field of fractions $\mathbb{K}(\mathcal{H})$ of $\mathbb{K}[\mathcal{H}]$. For a polynomial R in $\mathbb{K}[\mathcal{H}]$, the divisor of R is defined by $\mathrm{div}(R) = \sum_{P \in \mathcal{H}} \mathrm{ord}_P(R) P$, where $\mathrm{ord}_P(R)$ is the order of vanishing of R at P. For a rational function $R = F/G$,

where F, $G \in \mathbb{K}[\mathcal{H}]$, the divisor of R is defined by $\mathrm{div}(R) = \mathrm{div}(F) - \mathrm{div}(G)$ and is called a *principal divisor*. The *group of principal divisors* on $\mathcal{H}$ *over* $\mathbb{K}$ is denoted by $\mathcal{P}_{\mathcal{H}}(\mathbb{K}) = \{\mathrm{div}(R) : R \in \mathbb{K}(\mathcal{H})\}$. Specially $\mathcal{P}_{\mathcal{H}} = \mathcal{P}_{\mathcal{H}}(\overline{\mathbb{K}})$ is called the *group of principal divisors* on $\mathcal{H}$.

Definition 3. *The* Jacobian *of* $\mathcal{H}$ over $\mathbb{K}$ *is defined by*

$$J_{\mathcal{H}}(\mathbb{K}) = Div^0_{\mathcal{H}}(\mathbb{K})/\mathcal{P}_{\mathcal{H}}(\mathbb{K}).$$

Similarly, the Jacobian *of* $\mathcal{H}$ *is defined by* $J_{\mathcal{H}} = Div^0_{\mathcal{H}}/\mathcal{P}_{\mathcal{H}}$.

For each nontrivial class of divisors in $J_{\mathcal{H}}(\mathbb{K})$, there exist a unique divisor D on $\mathcal{H}$ over $\mathbb{K}$ of the form

$$D = \sum_{i=1}^{r} P_i - rP_\infty,$$

where $P_i = (x_i, y_i) \neq P_\infty$, $P_i \neq -P_j$, for $i \neq j$, and $r \leq g$. Such a divisor is called a *reduced* divisor on $\mathcal{H}$ over $\mathbb{K}$. By using Mumford's representation [19], each reduced divisor D on $\mathcal{H}$ over $\mathbb{K}$ can be uniquely represented by a pair of polynomials $[u(x), v(x)]$, $u, v \in \mathbb{K}[x]$, where u is monic, $\deg(v) < \deg(u) \leq g$, and $u \mid (v^2 - f)$. Precisely $u(x) = \prod_{i=1}^{r}(x - x_i)$ and $v(x_i) = y_i$. The neutral element of $J_{\mathcal{H}}(\mathbb{K})$, denoted by $\mathcal{O}$, is represented by $[1, 0]$. Cantor's algorithm, [3], efficiently computes the sum of two reduced divisors in $J_{\mathcal{H}}(\mathbb{K})$ and expresses it in reduced form.

2.4 Kummer Surface

Let H be an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$, for odd q. Then H has a plane model of the form

$$\mathbf{y}^2 = f(\mathbf{x}) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \tag{1}$$

where $f_i \in \mathbb{F}_q$ and f is a square-free polynomial. Then for the curve H, there exist a quartic surface $\mathcal{K}$ in $\mathbb{P}^3$, called the Kummer surface, which is given by the equation

$$A(k_1, k_2, k_3)k_4^2 + B(k_1, k_2, k_3)k_4 + C(k_1, k_2, k_3) = 0,$$

where

$$\begin{aligned}
A(k_1, k_2, k_3) =& k_2^2 - 4k_1k_3,\\
B(k_1, k_2, k_3) =& -2(2f_0k_1^3 + f_1k_1^2k_2 + 2f_2k_1^2k_3 + f_3k_1k_2k_3 + 2f_4k_1k_3^2 + k_2k_3^2),\\
C(k_1, k_2, k_3) =& -4f_0f_2k_1^4 + f_1^2k_1^4 - 4f_0f_3k_1^3k_2 - 2f_1f_3k_1^3k_3 - 4f_0f_4k_1^2k_2^2\\
&+ 4f_0k_1^2k_2k_3 - 4f_1f_4k_1^2k_2k_3 + 2f_1k_1^2k_3^2 - 4f_2f_4k_1^2k_3^2 + f_3^2k_1^2k_3^2\\
&- 4f_0k_1k_2^3 - 4f_1k_1k_2^2k_3 - 4f_2k_1k_2k_3^2 - 2f_3k_1k_3^3 + k_3^4.
\end{aligned}$$

Let $J(\mathbb{F}_q)$ be the Jacobian of H over $\mathbb{F}_q$ (see Subsection 2.3). Then there is a map

$$\kappa : J(\mathbb{F}_q) \longrightarrow \mathcal{K}(\mathbb{F}_q),$$

where $\kappa(D) = \kappa(-D)$, for all $D \in J(\mathbb{F}_q)$ and $\kappa(\mathcal{O}) = (0, 0, 0, 1)$. This map does not preserve the group structure, however, endows a pseudo-group structure on $\mathcal{K}$ (see [4]). In particular, a scalar multiplication on the image of κ is defined by

$$m\kappa(D) = \kappa(mD),$$

for $m \in \mathbb{Z}$ and $D \in J(\mathbb{F}_q)$. It could be used for a Diffie-Hellman protocol (see [21]). Furthermore, the above definition can be extended to have a scalar multiplication on $\mathcal{K}$. Since each point on $\mathcal{K}$ can be pulled back to the Jacobian of H or to the Jacobian of the quadratic twist of H.

2.5 Deterministic Extractor

In our analysis we use the notion of a deterministic extractor, so let us recall it briefly. For general definition of extractors we refer to [20,22].

Definition 4. *Let X and Y be S-valued random variables, where S is a finite set. Then the* statistical distance *$\Delta(X, Y)$ of X and Y is*

$$\Delta(X, Y) = \tfrac{1}{2} \textstyle\sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]| .$$

Let U_S denote a random variable uniformly distributed on S. We say that a random variable X on S is δ-uniform*, if $\Delta(X, U_S) \leq \delta$.*

Note that if the random variable X is *δ-uniform*, then no algorithm can distinguish X from U_S with advantage larger than δ, that is, for all algorithms $\mathcal{D} : S \longrightarrow \{0, 1\}$

$$|\Pr[\mathcal{D}(X) = 1] - \Pr[\mathcal{D}(U_S) = 1]| \leq \delta.$$

See [18].

Definition 5. *Let S, T be finite sets. Consider the function* $\mathrm{Ext} : S \longrightarrow T$*. We say that* Ext *is a* deterministic (T, δ)-extractor *for S if* $\mathrm{Ext}(U_S)$ *is δ-uniform on T. That means*

$$\Delta(\mathrm{Ext}(U_S), U_T) \leq \delta.$$

In the case that $T = \{0, 1\}^k$, we say Ext *is a* δ-deterministic extractor *for S.*

In this paper we consider deterministic $(\mathbb{F}_q, \delta)$-extractors. Observe that, converting random elements of $\mathbb{F}_q$ into random bit strings is a relatively easy problem. For instance, one can represent an element of $\mathbb{F}_q$ by a number in $\mathbb{Z}_q$ and convert this number to a bit-string of a length equal or very close to the bit length of q (e.g. see [13]). Furthermore, if q is close to a power of 2, that is, $0 \leq (2^n - q)/2^n \leq \delta$ for a small δ, then the uniform element $U_{\mathbb{F}_q}$ is statistically close to n uniformly random bits. The following simple lemma is a well-known result (the proof can be found, for instance, in [5]).

Lemma 1. *Under the condition that $0 \leq (2^n - q)/2^n \leq \delta$, the statistical distance between $U_{\mathbb{F}_q}$ and U_{2^n} is bounded from above by δ.*

3 Extractors for Jacobian

In this section we propose two extractors for the Jacobian of a hyperelliptic curve of genus 2 in odd characteristic. Then we analyse them.

We recall that H is an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$, for odd q, and $J(\mathbb{F}_q)$ is the Jacobian of H over $\mathbb{F}_q$. The hyperelliptic curve H has a plane model of the form $\mathbf{y}^2 = f(\mathbf{x})$, where f is a monic square-free polynomial of degree 5 (see equation (1)).

3.1 Sum Extractor for Jacobian

Definition 6. *The sum extractor* $\mathtt{SEJ}$ *for the Jacobian of* H *over* $\mathbb{F}_q$ *is defined as the function* $\mathtt{SEJ} : J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, *by*

$$\mathtt{SEJ}(D) = \begin{cases} \sum_{i=1}^{r} x_{P_i} & \text{if } D = \sum_{i=1}^{r} P_i - rP_\infty,\ 1 \le r \le 2 \\ 0 & \text{if } D = \mathcal{O}. \end{cases}$$

Remark 1. By using Mumford's representation for the points of $J(\mathbb{F}_q)$, the function $\mathtt{SEJ}$ is defined as

$$\mathtt{SEJ}(D) = \begin{cases} -u_1 & \text{if } D = [x^2 + u_1 x + u_0, v_1 x + v_0], \\ -u_0 & \text{if } D = [x + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

The following theorem gives the estimates for $\#\mathtt{SEJ}^{-1}(a)$, for all a in $\mathbb{F}_q$. In Subsection 3.3, we use the result of this theorem to analyse the extractor $\mathtt{SEJ}$. We give a proof of Theorem 2 in Section 4.

Theorem 2. *For all* $a \in \mathbb{F}_q^*$,

$$\left|\#\mathtt{SEJ}^{-1}(a) - q\right| \le 8\sqrt{q} + 1$$

and

$$\left|\#\mathtt{SEJ}^{-1}(0) - (q+1)\right| \le 8\sqrt{q} + 1.$$

3.2 Product Extractor for Jacobian

Definition 7. *The product extractor* $\mathtt{PEJ}$ *for the Jacobian of* H *over* $\mathbb{F}_q$ *is defined as the function* $\mathtt{PEJ} : J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, *by*

$$\mathtt{PEJ}(D) = \begin{cases} \prod_{i=1}^{r} x_{P_i} & \text{if } D = \sum_{i=1}^{r} P_i - rP_\infty,\ 1 \le r \le 2 \\ 0 & \text{if } D = \mathcal{O}. \end{cases}$$

Remark 2. By using Mumford's representation for the points of $J(\mathbb{F}_q)$, the function $\mathtt{PEJ}$ is defined as

$$\mathtt{PEJ}(D) = \begin{cases} u_0 & \text{if } D = [x^2 + u_1 x + u_0, v_1 x + v_0], \\ -u_0 & \text{if } D = [x + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

The next theorem shows the estimates for $\#\mathtt{PEJ}^{-1}(b)$, for all b in $\mathbb{F}_q$.

Theorem 3. *Let $b \in \mathbb{F}_q^*$. Let $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Then*

$$\left|\#\mathtt{PEJ}^{-1}(b) - q\right| \leq \begin{cases} 8\sqrt{q}+3 & \text{if } f_0 \neq 0, \\ 6\sqrt{q}+3 & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q+4\sqrt{q} & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

For $b = 0$,

$$\left|\#\mathtt{PEJ}^{-1}(0) - (eq+1)\right| \leq 4e\sqrt{q}\,,$$

where $e = \#\{(x,y) \in H(\mathbb{F}_q) : x = 0\}$.

3.3 Analysis of the Extractors

In this subsection we show that provided the divisor D is chosen uniformly at random in $J(\mathbb{F}_q)$, the element extracted from the divisor D by SEJ or PEJ is indistinguishable from a uniformly random element in $\mathbb{F}_q$.

Let $\mathtt{A}$ be a $\mathbb{F}_q$-valued random variable that is defined as

$$\mathtt{A} = \mathtt{SEJ}(D), \quad \text{for} \quad D \in_R J(\mathbb{F}_q).$$

Proposition 1. *The random variable $\mathtt{A}$ is statistically close to the uniform random variable $U_{\mathbb{F}_q}$.*

$$\Delta(\mathtt{A}, U_{\mathbb{F}_q}) = O(\frac{1}{\sqrt{q}}).$$

Proof. Let $a \in \mathbb{F}_q$. For the uniform random variable $U_{\mathbb{F}_q}$, $\Pr[U_{\mathbb{F}_q} = a] = 1/q$. Also for the $\mathbb{F}_q$-valued random variable $\mathtt{A}$,

$$\Pr[\mathtt{A} = a] = \frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)}.$$

The genus of H is 2, so by Hasse-Weil's Theorem we have

$$(\sqrt{q}-1)^4 \leq \#J(\mathbb{F}_q) \leq (\sqrt{q}+1)^4.$$

Theorem 2 gives the bound for $\#\mathtt{SEJ}^{-1}(a)$, for all $a \in \mathbb{F}_q$. Hence

$$\begin{aligned} \Delta(\mathtt{A}, U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{a\in\mathbb{F}_q} \left|\Pr[\mathtt{A} = a] - \Pr[U_{\mathbb{F}_q} = a]\right| \\ =& \frac{1}{2}\sum_{a\in\mathbb{F}_q} \left|\frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)} - \frac{1}{q}\right| \\ =& \frac{\left|q\#\mathtt{SEJ}^{-1}(0) - \#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)} + \sum_{a\in\mathbb{F}_q^*} \frac{\left|q\#\mathtt{SEJ}^{-1}(a) - \#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)}. \end{aligned}$$

Then

$$\begin{aligned}\Delta(\mathbb{A}, U_{\mathbb{F}_q}) \leq & \frac{(12q\sqrt{q} - 4q + 4\sqrt{q} - 1) + (q-1)(12q\sqrt{q} - 5q + 4\sqrt{q} - 1)}{2q(\sqrt{q}-1)^4} \\ = & \frac{12q\sqrt{q} - 5q + 4\sqrt{q}}{2(\sqrt{q}-1)^4} = \frac{6 + \epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{43q\sqrt{q} - 68q + 48\sqrt{q} - 12}{2(\sqrt{q}-1)^4}$. If $q \geq 570$, then $\epsilon(q) < 1$. □

Corollary 1. SEJ *is a deterministic* $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$*-extractor for* $J(\mathbb{F}_q)$.

Proof. Proposition 1 concludes the proof of this corollary. □

Corollary 2. PEJ *is a deterministic* $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$*-extractor for* $J(\mathbb{F}_q)$.

Proof. The result of Theorem 3 implies the proof of this corollary. □

4 Proofs of Theorems 2 and 3

In this section we give the proofs of Theorems 2 and 3. In other words, we are going to count the cardinalities of $\#\mathtt{SEJ}^{-1}(a)$, $\#\mathtt{PEJ}^{-1}(b)$, for all $a, b \in \mathbb{F}_q$. In Subsection 4.1, we recall some notes on the Jacobian of H over $\mathbb{F}_q$. We give the proof of Theorem 2 in Subsection 4.2. Then, we sketch the proof of Theorem 3 in Subsection 4.3.

4.1 Notes on the Jacobian of H over $\mathbb{F}_q$

We recall from Section 3 that $J(\mathbb{F}_q)$ is the Jacobian of H over $\mathbb{F}_q$. We partition $J(\mathbb{F}_q)$ as $J(\mathbb{F}_q) = J_0 \cup J_1 \cup J_2$, where $J_0 = \{\mathcal{O}\}$ and J_r, for $r = 1, 2$ is defined as

$$J_r = \{D \in J(\mathbb{F}_q) : D = [u(x), v(x)], deg(u) = r\}.$$

Recall that $\mathcal{O}$ is represented by $[1, 0]$.

Note that D is defined over $\mathbb{F}_q$, that means for all automorphisms φ in the Galois group of $\mathbb{F}_q$, $\varphi(D) = D$.

Let $D \in J_1$, then $D = P - P_\infty$, where $P = (x_P, y_P) \in H(\mathbb{F}_q)$. The Mumford's representation for D is $[x - x_P, y_P]$.

Let $D \in J_2$, then $D = P + Q - 2P_\infty$, where $P, Q \neq P_\infty$ and $P \neq -Q$. The divisor D is represented by $[u(x), v(x)]$, such that $u(x) = (x - x_P)(x - x_Q)$ and v is the line through P and Q. Since D is defined over $\mathbb{F}_q$, then $\phi(D) = \phi(P) + \phi(Q) - 2\phi(P_\infty) = D$, where ϕ is the Frobenius map. There are two cases for D.

- Suppose $\phi(P) = P$. Since $\phi(D) = D$, then $\phi(Q) = Q$. Thus P, $Q \in H(\mathbb{F}_q)$. That means

  $$D = P + Q - 2P_\infty,\ P, Q \in H(\mathbb{F}_q),\ P, Q \neq P_\infty, P \neq -Q.$$

  In this case the polynomial u is reducible over $\mathbb{F}_q$.

– Suppose $\phi(P) \neq P$. Since $\phi(D) = D$, so $\phi(P) = Q$ and $\phi(Q) = P$. Then $\phi(\phi(P)) = P$. Hence $P \in H(\mathbb{F}_{q^2})$. That means

$$D = P + \phi(P) - 2P_\infty,\ P \in H(\mathbb{F}_{q^2}),\ P \neq P_\infty, \phi(P) \neq \pm P.$$

In this case the polynomial u is irreducible over $\mathbb{F}_q$.

Let

$$\mathcal{J} = \{(P,Q) : P,Q \in H(\mathbb{F}_q),\ P,Q \neq P_\infty, Q \neq -P\},$$
$$\mathcal{J}^\phi = \{(P,\phi(P)) : P \in H(\mathbb{F}_{q^2}), P \neq P_\infty,\ \phi(P) \neq -P\}.$$

Lemma 2. *Let $\sigma : \mathcal{J} \longrightarrow J_2$ be the map defined by*

$$\sigma(P,Q) = P + Q - 2P_\infty,$$

and let $\sigma_\phi : \mathcal{J}^\phi \longrightarrow J_2$ be the map defined by

$$\sigma_\phi(P,\phi(P)) = P + \phi(P) - 2P_\infty.$$

Then $\#\sigma^{-1}(D) + \#\sigma_\phi^{-1}(D) = 2$, for all $D \in J_2$.

Proof. Let $D \in J_2$. Then we have the following cases.

1. Assume $D = P + Q - 2P_\infty$, such that $P,Q \in H(\mathbb{F}_q)$, $P,Q \neq P_\infty$ and $Q \neq P$. Clearly $\sigma^{-1}(D) = \{(P,Q),(Q,P)\}$ and $\sigma_\phi^{-1}(D) = \emptyset$.
2. Assume $D = P + \phi(P) - 2P_\infty$, such that $P \in H(\mathbb{F}_{q^2})$, $P \neq P_\infty$ and $\phi(P) \neq P$. Clearly $\sigma^{-1}(D) = \emptyset$ and $\sigma_\phi^{-1}(D) = \{(P,\phi(P)),(\phi(P),P)\}$.
3. Assume $D = 2P - 2P_\infty$, where $P \in H(\mathbb{F}_q)$, $P \neq P_\infty$. It is easy to see that $\sigma^{-1}(D) = \sigma_\phi^{-1}(D) = \{(P,P)\}$. □

4.2 Proof of Theorem 2

For the proof of Theorem 2, we need several propositions. First, by Proposition 2, we transform our problem to the problem of computing sum of the cardinalities of corresponding sets in Definition 8. Second, in proposition 3, we give a formula for this sum in terms of the cardinalities of some curves. Finally, by using Hasse-Weil Theorem, we obtain tight estimates for $\#\mathtt{SEJ}^{-1}(a)$, for all $a \in \mathbb{F}_q$.

Definition 8. *Let $a \in \mathbb{F}_q$. Define*

$$\Sigma_a = \{(P,Q) : P,Q \in H(\mathbb{F}_q),\ x_P + x_Q = a\},$$
$$\Sigma_a^\phi = \{(P,\phi(P)) : P \in H(\mathbb{F}_{q^2}),\ x_P + x_{\phi(P)} = a\}.$$

Proposition 2. *For all $a \in \mathbb{F}_q$,*

$$\#(\mathtt{SEJ}^{-1}(a) \cap J_2) = \frac{\#\Sigma_a + \#\Sigma_a^\phi}{2} - 1.$$

Proof. Let $a \in \mathbb{F}_q$. Let $\mathcal{S}_a = \sigma^{-1}(\mathtt{SEJ}^{-1}(a) \cap J_2)$ and $\mathcal{S}_a^\phi = \sigma_\phi^{-1}(\mathtt{SEJ}^{-1}(a) \cap J_2)$ (see Lemma 2). Then $\Sigma_a = \mathcal{S}_a \cup \mathcal{E}_a$ and $\Sigma_a^\phi = \mathcal{S}_a^\phi \cup \mathcal{E}_a^\phi$, where $\mathcal{E}_a = \{(P,Q) : (P,Q) \in \Sigma_a, Q = -P\}$ and $\mathcal{E}_a^\phi = \{(P,\phi(P)) : (P,\phi(P)) \in \Sigma_a^\phi, \phi(P) = -P\}$. Since $\mathcal{S}_a$ and $\mathcal{E}_a$ are disjoint, so $\#\Sigma_a = \#\mathcal{S}_a + \#\mathcal{E}_a$. Similarly, $\#\Sigma_a^\phi = \#\mathcal{S}_a^\phi + \#\mathcal{E}_a^\phi$.

Assume $(P,-P)$ is a point of $\mathcal{E}_a$ or $\mathcal{E}_a^\phi$, then $x_P = \frac{a}{2}$. Obviously P is a point of $H(\mathbb{F}_q)$ or $H(\mathbb{F}_{q^2})$. Suppose $f(\frac{a}{2}) = 0$. Then $P \in H(\mathbb{F}_q)$ and $P = -P$. That means $\mathcal{E}_a = \mathcal{E}_a^\phi = \{(P,P)\}$. Now, suppose $f(\frac{a}{2}) \neq 0$. So $P \neq -P$. If $P \in H(\mathbb{F}_q)$, then $\mathcal{E}_a = \{(P,-P),(-P,P)\}$ and $\mathcal{E}_a^\phi = \emptyset$. Otherwise, P is a point of $H(\mathbb{F}_{q^2})$. Thus $\phi(P) = -P$. Hence $\mathcal{E}_a = \emptyset$ and $\mathcal{E}_a^\phi = \{(P,-P),(-P,P)\}$. In other words $\#\mathcal{E}_a + \#\mathcal{E}_a^\phi = 2$.

Lemma 2 implies that $\#\mathcal{S}_a + \#\mathcal{S}_a^\phi = 2\#(\mathtt{SEJ}^{-1}(a) \cap J_2)$. That concludes the proof of this proposition. □

Proposition 2 gives the estimate for the cardinality of $\mathtt{SEJ}^{-1}(a)$, for $a \in \mathbb{F}_q$, in terms of the sum of the cardinalities of Σ_a and Σ_a^ϕ. Now, we are dealing to have a tight estimate for $\#\Sigma_a + \#\Sigma_a^\phi$, for all $a \in \mathbb{F}_q$. In order to do that, we define a curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q$. Then, in Proposition 3, we give a formula for $\#\Sigma_a + \#\Sigma_a^\phi$ in terms of the cardinalities of $H(\mathbb{F}_q)$ and $\mathcal{X}_a(\mathbb{F}_q)$. After that, using the Hasse-Weil's Theorem, we obtain a tight estimate for $\#\Sigma_a + \#\Sigma_a^\phi$.

The hyperellitic curve H has the plane model defined by

$$\mathbf{y}^2 = f(\mathbf{x}) = \prod_{i=1}^{5}(\mathbf{x} - \lambda_i), \tag{2}$$

where λ_i are pairwise distinct elements of $\overline{\mathbb{F}}_q$. (see equation (1)). Define the two-variable polynomial $\Phi \in \mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1]$ as $\Phi(\mathbf{x}_0, \mathbf{x}_1) = f(\mathbf{x}_0)f(\mathbf{x}_1)$. Clearly Φ is a symmetric polynomial. Let $\mathbf{a} = \mathbf{x}_0 + \mathbf{x}_1$ and $\mathbf{b} = \mathbf{x}_0\mathbf{x}_1$. Then from equation (2), we obtain

$$\Phi(\mathbf{x}_0, \mathbf{x}_1) = \prod_{i=1}^{5}((\mathbf{x}_0 - \lambda_i)(\mathbf{x}_1 - \lambda_i)) = \prod_{i=1}^{5}(\mathbf{x}_0\mathbf{x}_1 - \lambda_i(\mathbf{x}_0 + \mathbf{x}_1) + \lambda_i^2)$$

Define the two-variable polynomial Ψ in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ by

$$\Psi(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^{5}(\mathbf{b} - \lambda_i\mathbf{a} + \lambda_i^2). \tag{3}$$

For $a \in \mathbb{F}_q$, let $\mathcal{X}_a$ be the affine curve defined over $\mathbb{F}_q$, by the equation

$$\mathbf{y}^2 = \Psi_a(\mathbf{b}) = \Psi(a, \mathbf{b}). \tag{4}$$

Proposition 3. *Let $a \in \mathbb{F}_q$. Then*

$$\#\Sigma_a + \#\Sigma_a^\phi = 2(\#H(\mathbb{F}_q) + \#\mathcal{X}_a(\mathbb{F}_q) - q - 1).$$

Proof. See Proposition 12. □

Clearly the affine curve $\mathcal{X}_a$ is absolutely irreducible, for all $a \in \mathbb{F}_q$. The curve $\mathcal{X}_a$ is nonsingular for almost all $a \in \mathbb{F}_q$. Furthermore, the genus of the nonsingular model of $\mathcal{X}_a$ is at most 2. By using the Hasse-Weil's bound for the nonsingular model of $\mathcal{X}_a$, we obtain an estimate for $\#\mathcal{X}_a(\mathbb{F}_q)$.

Proposition 4. *For all $a \in \mathbb{F}_q$,*

$$|\#\mathcal{X}_a(\mathbb{F}_q) - q| \leq 4\sqrt{q}.$$

Proof. See Subsection B.1. □

Proof (Theorem 2). Let $a \in \mathbb{F}_q$. Proposition 2 shows that

$$\#(\mathtt{SEJ}^{-1}(a) \cap J_2) = \frac{\#\Sigma_a + \#\Sigma_a^{\phi}}{2} - 1.$$

From Proposition 3, we have

$$\#\Sigma_a + \#\Sigma_a^{\phi} = 2(\#H(\mathbb{F}_q) + \#\mathcal{X}_a(\mathbb{F}_q) - q - 1).$$

Then by using Hasse-Weil's bound for H we obtain

$$|\#H(\mathbb{F}_q) - q - 1| \leq 4\sqrt{q}.$$

Furthermore, from Proposition 4 we have

$$|\#\mathcal{X}_a(\mathbb{F}_q) - q| \leq 4\sqrt{q}.$$

Hence

$$\big|\#(\mathtt{SEJ}^{-1}(a) \cap J_2) - q\big| \leq 8\sqrt{q}.$$

Clearly $\#(\mathtt{SEJ}^{-1}(a) \cap J_1)$ equals $0, 1$ or 2. If $a = 0$, then $\#(\mathtt{SEJ}^{-1}(a) \cap J_0)$ equals 1, otherwise equals 0. So the proof of Theorem 2 is completed. □

4.3 Proof of Theorem 3

The proof of Theorem 3 is similar to the proof of Theorem 2. First, in Proposition 5, we give the estimate for the cardinality of $\mathtt{PEJ}^{-1}(b)$, for $b \in \mathbb{F}_q^*$, in terms of the sum of the cardinalities of Π_b and Π_b^{ϕ}. Second, in Proposition 6, we give a relation between $\#\Sigma_a + \#\Sigma_a^{\phi}$ and the cardinalities of $\mathcal{H}(\mathbb{F}_q)$ and $\mathcal{X}_a(\mathbb{F}_q)$. Finally, Hasse-Weil Theorem concludes the proof of Theorem 3.

Definition 9. *Let $b \in \mathbb{F}_q^*$. Define*

$$\Pi_b = \{(P, Q) : P, Q \in H(\mathbb{F}_q),\ x_P x_Q = b\},$$
$$\Pi_b^{\phi} = \{(P, \phi(P)) : P \in H(\mathbb{F}_{q^2}),\ x_P x_{\phi(P)} = b\}.$$

Proposition 5. *For all $b \in \mathbb{F}_q^*$,*

$$\#(\mathtt{PEJ}^{-1}(b) \cap J_2) = \frac{\#\Pi_b + \#\Pi_b^{\phi}}{2} - r_b,$$

where r_b equals the number of square roots of b in $\mathbb{F}_q^*$.

Proof. The proof of this proposition is similar to the proof of Proposition 2. So we leave it for the interested reader. □

Consider the polynomial $\Psi \in \mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ defined by the equation (3). Let $\mathcal{X}_b$ be the affine curve defined over $\mathbb{F}_q$, by the equation

$$\mathbf{y}^2 = \Psi_b(\mathbf{a}) = \prod_{i=1}^{5}(b - \lambda_i \mathbf{a} + \lambda_i^2), \tag{5}$$

for $b \in \mathbb{F}_q^*$.

Proposition 6. *Let $b \in \mathbb{F}_q^*$. Then*

$$\#\Pi_b + \#\Pi_b^{\phi} = 2(\#H(\mathbb{F}_q) + \#\mathcal{X}_b(\mathbb{F}_q) - q - e),$$

where $e = \#\{(x, y) \in H(\mathbb{F}_q) : x = 0\}$.

Proof. The proof of this proposition is similar to the proof of Proposition 3. □

The affine curve $\mathcal{X}_b$ is absolutely irreducible and nonsingular, for almost all $b \in \mathbb{F}_q$. In fact the curve $\mathcal{X}_b$ is reducible if and only if $\lambda_i = 0$, for some i, and $b \in I_f$, where $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Provided the curve $\mathcal{X}_b$ is absolutely irreducible, the genus of the nonsingular model of $\mathcal{X}_b$ is at most 2. Then Hasse-Weil's Theorem gives the estimates for $\#\mathcal{X}_b(\mathbb{F}_q)$.

Proposition 7. *Let $b \in \mathbb{F}_q$. Then*

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq \begin{cases} 4\sqrt{q} & \text{if } f_0 \neq 0, \\ 2\sqrt{q} & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

Proof. See Subsection B.2. □

Proof (Theorem 3). Let $b \in \mathbb{F}_q^*$. Proposition 5 shows that

$$\#(\mathtt{PEJ}^{-1}(b) \cap J_2) = \frac{\#\Pi_b + \#\Pi_b^{\phi}}{2} - r_b,$$

where r_b equals the number of square roots of b in $\mathbb{F}_q$. It is easy to see that $0 \leq \#(\mathtt{PEJ}^{-1}(b) \cap J_1) \leq 2$ and $\#(\mathtt{PEJ}^{-1}(b) \cap J_0) = 0$. So

$$\left|\#\mathtt{PEJ}^{-1}(b) - q\right| \leq \frac{\left|\#\Pi_b + \#\Pi_b^{\phi} - 2q\right|}{2} + 2.$$

From Proposition 6, we have

$$\#\Pi_b + \#\Pi_b^{\phi} = 2(\#H(\mathbb{F}_q) + \#\mathcal{X}_b(\mathbb{F}_q) - q - e),$$

where e is the number of points on $H(\mathbb{F}_q)$ whose abscissa equals zero. Note that $0 \leq e \leq 2$. Hence

$$\left|\#\Pi_b + \#\Pi_b^{\phi} - 2q\right| \leq 2\left|\#H(\mathbb{F}_q) + \#\mathcal{X}_b(\mathbb{F}_q) - 2q - 1\right| + 2.$$

Hasse-Weil's Theorem gives the bound for $\#H(\mathbb{F}_q)$. Then Proposition 7 concludes the proof of Theorem 3 for all $b \in \mathbb{F}_q^*$.

Now assume that $b = 0$. It is easy to see $\#\mathtt{PEJ}^{-1}(0) = e\#H(\mathbb{F}_q) - e + 1$, where e equals the number of points of $H(\mathbb{F}_q)$ whose abscissa equals zero. So the proof of Theorem 3 is completed. □

5 Extractors for Kummer Surface

Consider the hyperelliptic curve H that is defined in equation (1). Let $\mathcal{K}$ be the Kummer surface related to $J(\mathbb{F}_q)$ (Jacobian of H over $\mathbb{F}_q$). We recall that each point of $J(\mathbb{F}_q)$ can be uniquely represented by at most 2 points on H. Then there is a map

$$\begin{aligned} \kappa : J(\mathbb{F}_q) &\longrightarrow \mathcal{K}(\mathbb{F}_q) \\ P + Q - 2P_\infty &\longmapsto (1 : a : b : c) \\ P - P_\infty &\longmapsto (0 : 1 : x_P : x_P^2) \\ \mathcal{O} &\longmapsto (0 : 0 : 0 : 1), \end{aligned}$$

where $a = x_P + x_Q$, $b = x_P x_Q$ and

$$c = \begin{cases} \dfrac{\widetilde{B}(a,b) - 2y_P y_Q}{(x_P - x_Q)^2} & \text{if } P \neq Q \\ \dfrac{\widetilde{C}(a,b)}{4y_P^2} & \text{if } P = Q, \end{cases}$$

with

$$\begin{aligned} \widetilde{B}(a,b) &= ab^2 + f_3 ab + f_1 a + 2f_4 b^2 + 2f_2 b + 2f_0, \\ \widetilde{C}(a,b) &= C(1,a,b). \end{aligned}$$

5.1 Sum Extractor for Kummer Surface

In this subsection we define the *sum extractor* SEK for the Kummer surface $\mathcal{K}$. Then we define the *sum extractor* SEKJ as the restriction of SEK to the image of κ. We briefly mention the analysis of these extractors.

Definition 10. *The sum extractor* SEK *for the Kummer surface* $\mathcal{K}$ *is defined as the function* $\mathtt{SEK} : \mathcal{K}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, *by*

$$\mathtt{SEK}(k_1 : k_2 : k_3 : k_4) = \begin{cases} \dfrac{k_2}{k_1} & \text{if } k_1 \neq 0, \\ \dfrac{k_3}{k_2} & \text{if } k_1 = 0, k_2 \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The following theorem gives the estimates for $\#\mathtt{SEK}^{-1}(a)$, for all a in $\mathbb{F}_q$. By using the result of this theorem, one can show that SEK is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\mathcal{K}(\mathbb{F}_q)$.

Theorem 4. *For all* $a \in \mathbb{F}_q^*$,

$$\left|\#\mathtt{SEK}^{-1}(a) - q\right| \leq 4\sqrt{q}$$

and

$$\left|\#\mathtt{SEK}^{-1}(0) - (q+1)\right| \leq 4\sqrt{q}.$$

Proof. Note that each point on $\mathcal{K}$ can be pulled back to the Jacobian of H or to the Jacobian of the quadratic twist of H. Furthermore, the map κ is $2:1$ on all points except the points of order 2 in the Jacobian of H where it is $1:1$. Then, the proof of Theorem 2 and the application of that proof for the sum extractor for the Jacobian of the quadratic twist of H conclude the proof of this Theorem. □

The scalar multiplication on $\kappa(J(\mathbb{F}_q))$ could be used for a variant of Diffie-Hellman protocol on this set. For instance, consider the case that $J(\mathbb{F}_q)$ is a cyclic group with generator D_g. Then $\kappa(D_g)$ is the generator of $\kappa(J(\mathbb{F}_q))$. That brings us to define the following extractor for this set.

Definition 11. *The sum extractor* SEKJ *for* $\kappa(J(\mathbb{F}_q))$*, is defined as the restriction of the extractor* SEK *to* $\kappa(J(\mathbb{F}_q))$.

The following theorem shows that $\#\mathtt{SEJ}^{-1}(a) = 2\#\mathtt{SEKJ}^{-1}(a)$, for almost all $a \in \mathbb{F}_q$. One can show that SEKJ is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\kappa(J(\mathbb{F}_q))$ (see Subsection 3.3).

Proposition 8. *For all* $a \in \mathbb{F}_q$,

$$\#\mathtt{SEKJ}^{-1}(a) = \frac{\#\mathtt{SEJ}^{-1}(a) + d_a}{2},$$

where d_a *is the number of two torsion points of* $J(\mathbb{F}_q)$ *in* $\mathtt{SEJ}^{-1}(a)$.

Proof. The fact that the map κ is $2:1$ on all points except the points of order 2 in the Jacobian of H where it is $1:1$, concludes the proof of this proposition. □

Remark 3. It is easy to see that $0 \leq d_a \leq 3$ and $\sum_{a \in \mathbb{F}_q} d_a$ equals the number of two torsion points of $J(\mathbb{F}_q)$, which is bounded by 16.

5.2 Product Extractor for Kummer Surface

In this subsection we define the *product extractor* PEK for the $\mathcal{K}$. We briefly mention the analysis of this extractor.

Definition 12. *The product extractor* PEK *for the Kummer surface* $\mathcal{K}$ *is defined as the function* $\mathtt{PEK} : \mathcal{K}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$*, by*

$$\mathtt{PEK}(k_1 : k_2 : k_3 : k_4) = \begin{cases} \dfrac{k_3}{k_1} & \text{if } k_1 \neq 0, \\ \dfrac{k_3}{k_2} & \text{if } k_1 = 0, k_2 \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The next theorem gives the estimates for $\#\mathtt{PEK}^{-1}(b)$, for all b in $\mathbb{F}_q$. The result of this theorem implies that PEK is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\mathcal{K}(\mathbb{F}_q)$.

Theorem 5. *Let $b \in \mathbb{F}_q$. Let $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Then*

$$\left|\#\mathtt{PEK}^{-1}(b) - q\right| \leq \begin{cases} 4\sqrt{q}+1 & \text{if } f_0 \neq 0, \\ 2\sqrt{q}+1 & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q-1 & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

Furthermore, one can define the *product extractor* PEKJ for $\kappa(J(\mathbb{F}_q))$ as the restriction of the extractor PEK to $\kappa(J(\mathbb{F}_q))$.

6 Conclusion

We propose the *sum* and *product* extractors, SEJ and PEJ, for $J(\mathbb{F}_q)$, the Jacobian of a genus 2 hyperelliptic curve H over $\mathbb{F}_q$. We show that the outputs of these extractors, for a given uniformly random point of $J(\mathbb{F}_q)$, are statistically close to a uniformly random variable in $\mathbb{F}_q$. To show the latter we need some bounds on the cardinalities of $\mathtt{SEJ}^{-1}(a)$ and $\mathtt{PEJ}^{-1}(b)$, for all $a, b \in \mathbb{F}_q$. To have these estimates, we introduce some corresponding problems. In new problems, we are looking for bounds on the cardinality of some curves. We give our estimates in Theorems 2 and 3 using Hasse-Weil Theorem.

Thanks to the Kummer surface $\mathcal{K}$, that is associated to the Jacobian of H over $\mathbb{F}_q$, we propose the *sum* and *product* extractors, SEK and PEK, for $\mathcal{K}(\mathbb{F}_q)$. These extractors are the modified versions of the extractors SEJ and PEJ. Provided a point K is chosen uniformly at random in $\mathcal{K}$, the element extracted from the point K is statistically close to a uniformly random variable in $\mathbb{F}_q$.

Our proposed extractors can be generalized for the Jacobian of hyperelliptic curves of higher genus.

Acknowledgment. The author thanks to the anonymous referees for several useful suggestions.

References

1. Artin, E.: Algebraic Numbers and Algebraic Functions. Gordon and Breach, New York (1967)
2. Avanzi, R.M.: Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 148–162. Springer, Heidelberg (2004)
3. Cantor, D.: Computing in the Jacobian of a Hyperelliptic Curve. Mathematics of Computation 48(177), 95–101 (1987)
4. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2. Cambridge University Press, Cambridge (1996)
5. Chevassut, O., Fouque, P., Gaudry, P., Pointcheval, D.: The Twist-Augmented Technique for Key Exchange. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 410–426. Springer, Heidelberg (2006)

6. Cohen, H., Frey, G.: Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, New York (2006)
7. Duquesne, S.: Montgomery Scalar Multiplication for Genus 2 Curves. In: Buell, D.A. (ed.) ANTS 2004. LNCS, vol. 3076, pp. 153–168. Springer, Heidelberg (2004)
8. Farashahi, R.R., Pellikaan, R.: The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic. In: WAIFI 2007. LNCS, vol. 4547, pp. 219–236. Springer, Heidelberg (2007)
9. Farashahi, R.R., Pellikaan, R., Sidorenko, A.: Extractors for Binary Elliptic Curves. In: WCC 2007. Workshop on Coding and Cryptography, pp. 127–136 (2007)
10. Gaudry, P.: An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 3419–3448. Springer, Heidelberg (2000)
11. Gaudry, P.: Fast genus 2 arithmetic based on Theta functions, Cryptology ePrint Archive, Report 2005/314 (2005), http://eprint.iacr.org/
12. Gürel, N.: Extracting bits from coordinates of a point of an elliptic curve, Cryptology ePrint Archive, Report 2005/324 (2005), http://eprint.iacr.org/
13. Juels, A., Jakobsson, M., Shriver, E., Hillyer, B.K.: How to turn loaded dice into fair coins. IEEE Transactions on Information Theory 46(3), 911–921 (2000)
14. Kaliski, B.S.: A Pseudo-Random Bit Generator Based on Elliptic Logarithms. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 84–103. Springer, Heidelberg (1987)
15. Koblitz, N.: Hyperelliptic Cryptosystem. J. of Cryptology 1, 139–150 (1989)
16. Lange, T.: Montgomery Addition for Genus Two Curves. In: Buell, D.A. (ed.) ANTS 2004. LNCS, vol. 3076, pp. 307–309. Springer, Heidelberg (2004)
17. Lange, T.: Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. aaecc 15(1), 295–328 (2005)
18. Luby, M.: Pseudorandomness and Cryptographic Applications. Princeton University Press, USA (1994)
19. Mumford, D.: Tata Lectures on Theta II. In: Progress in Mathematics, vol. 43 (1984)
20. Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. Bulletin of the EATCS 77, 67–95 (2002)
21. Smart, N.P., Siksek, S.: A Fast Diffie-Hellman Protocol in Genus 2. Journal of Cryptology 12, 67–73 (1999)
22. Trevisan, L., Vadhan, S.: Extracting Randomness from Samplable Distributions. In: IEEE Symposium on Foundations of Computer Science, pp. 32–42 (2000)

Appendix

A Corresponding Problems

In this section we are dealing with computing the bounds for the cardinalities of Σ_a and Σ_a^ϕ, for $a \in \mathbb{F}_q$ (see Definition 8). We reconsider Definition 8 related to an affine curve with an arbitrary genus. In particular, the sum of Σ_a and Σ_a^ϕ are related to subsets of points of the Jacobian of a genus 2 hyperelliptic (see Proposition 2).

Let $\mathcal{C}$ be an affine curve that is defined over $\mathbb{F}_q$ by the equation

$$\mathbf{y}^2 = f(\mathbf{x}),$$

where $f(\mathbf{x}) \in \mathbb{F}_q[x]$ is a monic polynomial of a positive degree d. Let $a \in \mathbb{F}_q$. We recall that

$$\Sigma_a = \{(P,Q) : P,Q \in \mathcal{C}(\mathbb{F}_q),\ x_P + x_Q = a\},$$
$$\Sigma_a^{\phi} = \{(P,\phi(P)) : P \in \mathcal{C}(\mathbb{F}_{q^2}),\ x_P + x_{\phi(P)} = a\}.$$

Note that we reconsider Definition 8 that is now related to the affine curve $\mathcal{C}$.

A.1 Cardinality of Σ_a

For an element $a \in \mathbb{F}_q$, the set Σ_a includes the ordered pairs of points on $\mathcal{C}(\mathbb{F}_q)$, such that the sum of their abscissas equals a.

Let $\mathcal{C}_a$ be the affine curve defined over $\mathbb{F}_q$ by the equation

$$\mathbf{z}^2 = f_a(\mathbf{x}) = f(a - \mathbf{x}).$$

Let $\mathcal{C}_a^{\star}$ be the affine curve over $\mathbb{F}_q$, that is defined by the following equation.

$$\mathbf{w}^2 = f_a^{\star}(\mathbf{x}) = f(\mathbf{x})f(a - \mathbf{x}).$$

The next proposition gives a formula for the cardinality of Σ_a in terms of the numbers of $\mathbb{F}_q$-rational points of curves $\mathcal{C}$ and $\mathcal{C}_a^{\star}$.

Lemma 3. *Define*

$$T_a = \{(P,Q) : P \in \mathcal{C}(\mathbb{F}_q), Q \in \mathcal{C}_a(\mathbb{F}_q),\ x_P = x_Q\}.$$

Then $\#T_a = \#\Sigma_a$.

Proof. Clearly $((x,y),(x',y')) \in T$ if and only if $((x,y),(a-x',y')) \in \Sigma_a$. □

Lemma 4. *Define the function* $\pi_{T_a} : T_a \longrightarrow \mathbb{F}_q$ *by* $\pi_{T_a}(P,Q) = x_P$. *Define the projection map* $\pi_{\mathcal{C}} : \mathcal{C}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ *by* $\pi_{\mathcal{C}}(P) = x_P$. *Similarly define the projection maps* $\pi_{\mathcal{C}_a}$ *and* $\pi_{\mathcal{C}_a^{\star}}$, *for the curves* $\mathcal{C}_a$, $\mathcal{C}_a^{\star}$. *Then*

$$\#\pi_{\mathcal{C}}^{-1}(x) + \#\pi_{\mathcal{C}_a}^{-1}(x) + \#\pi_{\mathcal{C}_a^{\star}}^{-1}(x) = 2 + \#\pi_{T_a}^{-1}(x),$$

for all $x \in \mathbb{F}_q$.

Proof. Define $m(x) = \#\pi_{T_a}^{-1}(x)$ and $r(x) = \#\pi_{\mathcal{C}}^{-1}(x) + \#\pi_{\mathcal{C}_a}^{-1}(x) + \#\pi_{\mathcal{C}_a^{\star}}^{-1}(x)$, for $x \in \mathbb{F}_q$. We shall prove that $r(x) = 2 + m(x)$, for all $x \in \mathbb{F}_q$.

Let $x \in \mathbb{F}_q$. Let $X_{T_a} = \pi_{T_a}(T_a)$. First we assume that $x \in X_{T_a}$ and $f_a^{\star}(x) \neq 0$. Then there exist points $P = (x,y) \in \mathcal{C}(\mathbb{F}_q)$ and $Q = (x,z) \in \mathcal{C}_a(\mathbb{F}_q)$. Let $R = (x,w)$, where $w = yz$. So R is a point on $\mathcal{C}_a^{\star}(\mathbb{F}_q)$. Note that y, z and w are nonzero elements in $\mathbb{F}_q$. So $-P = (x,-y) \neq P$, also $-Q \neq Q$ and $-R \neq R$. Then it is easy to see that $\pi_{\mathcal{C}}^{-1}(x) = \{P,-P\}$, $\pi_{\mathcal{C}_a}^{-1}(x) = \{Q,-Q\}$ and $\pi_{\mathcal{C}_a^{\star}}^{-1}(x) = \{R,-R\}$. So $r(x) = 6$. Also $\pi_T^{-1}(x) = \{(P,Q),(P,-Q),(-P,Q),(-P,-Q)\}$. That means $m(x) = 4$.

Second we assume that $x \in \mathbb{F}_q \setminus X_{T_a}$ and $f_a^{\star}(x) \neq 0$. Since $x \notin X_{T_a}$, then $\pi_T^{-1}(x) = \emptyset$ and $m(x) = 0$. If there exist a point $P = (x,y) \in \mathcal{C}(\mathbb{F}_q)$ then

$\pi_{\mathcal{C}}^{-1}(x) = \{P, -P\}$ and $\pi_{\mathcal{C}_a}^{-1}(x) = \emptyset$, since $x \notin X_{T_a}$. Also $\pi_{\mathcal{C}_a^\star}^{-1}(x) = \emptyset$, since if there exist a point $R = (x, w) \in \mathcal{C}_a^\star(\mathbb{F}_q)$, then $(x, w/y) \in \mathcal{C}_a(\mathbb{F}_q)$, which contradicts the assumption that $x \notin X_{T_a}$. Hence $r(x) = 2$. Similarly if there exist a point $Q = (x, z) \in \mathcal{C}_a(\mathbb{F}_q)$, then $\pi_{\mathcal{C}_a}^{-1}(x) = \{Q, -Q\}$ and $\pi_{\mathcal{C}}^{-1}(x) = \pi_{\mathcal{C}_a^\star}^{-1}(x) = \emptyset$. That means $r(x) = 2$. Therefore assume that there do not exist points on $\mathcal{C}(\mathbb{F}_q)$ or $\mathcal{C}_a(\mathbb{F}_q)$, with the abscissa equals x. So $f(x)$ and $f_a(x)$ are not squared in $\mathbb{F}_q$. Hence $f_a^\star(x)$ is a squared in $\mathbb{F}_q$. Let w be the square root of $f_a^\star(x)$. Then $R = (x, z) \in \mathcal{C}_a^\star(\mathbb{F}_q)$. Therefore $\pi_{\mathcal{C}_a^\star}^{-1}(x) = \{R, -R\}$ and $\pi_{\mathcal{C}}^{-1}(x) = \pi_{\mathcal{C}_a}^{-1}(x) = \emptyset$. Thus $r(x) = 2$.

Third we assume that $x \in X_{T_a}$ and $f_a^\star(x) = 0$. So $\pi_{\mathcal{C}_a^\star}^{-1}(x) = \{P_0\}$, where $P_0 = (x, 0)$. Since $f_a^\star(x) = 0$, then $f(x) = 0$ or $f_a(x) = 0$. If both of $f(x)$ and $f_a(x)$ are zero, then $\pi_{\mathcal{C}}^{-1}(x) = \pi_{\mathcal{C}_a}^{-1}(x) = \{P_0\}$. Also $\pi_T^{-1}(x) = \{(P_0, P_0)\}$. Hence in this case $r(x) = 3$ and $m(x) = 1$. If $f(x) = 0$, but $f_a(x) \neq 0$, then there exist a point $Q = (x, z) \in \mathcal{C}_a(\mathbb{F}_q)$, where $z \neq 0$. Hence $\pi_{\mathcal{C}}^{-1}(x) = \{P_0\}$ and $\pi_{\mathcal{C}_a}^{-1}(x) = \{Q, -Q\}$. Also $\pi_T^{-1}(x) = \{(P_0, Q), (P_0, -Q)\}$. Therefore $r(x) = 4$ and $m(x) = 2$. Similarly in the case that $f(x) \neq 0$ and $f_a(x) = 0$, $r(x) = 4$ and $m(x) = 2$.

Finally we assume that $x \in \mathbb{F}_q \setminus X_{T_a}$ and $f_a^\star(x) = 0$. So $\pi_{\mathcal{C}_a^\star}^{-1}(x) = \{P_0\}$. If $f(x) = 0$, then $\pi_{\mathcal{C}}^{-1}(x) = \{P_0\}$ but $\pi_{\mathcal{C}_a}^{-1}(x) = \emptyset$, since $x \notin X_{T_a}$. Hence $r(x) = 2$ and $m(x) = 0$. If $f_a(x) = 0$, then $\pi_{\mathcal{C}}^{-1}(x) = \emptyset$ and $\pi_{\mathcal{C}_a}^{-1}(x) = \{P_0\}$. Therefore $r(x) = m(x) + 2$, for all $x \in \mathbb{F}_q$. □

Proposition 9. *For all $a \in \mathbb{F}_q$,*

$$\#\Sigma_a = 2\#\mathcal{C}(\mathbb{F}_q) + \#\mathcal{C}_a^\star(\mathbb{F}_q) - 2q.$$

Proof. From Lemma 4, we have

$$\begin{aligned}\#\mathcal{C}(\mathbb{F}_q) + \#\mathcal{C}_a(\mathbb{F}_q) + \#\mathcal{C}_a^\star(\mathbb{F}_q) &= \sum_{x \in \mathbb{F}_q} (\#\pi_{\mathcal{C}}^{-1}(x) + \#\pi_{\mathcal{C}_a}^{-1}(x) + \#\pi_{\mathcal{C}_a^\star}^{-1}(x)) \\ &= \sum_{x \in \mathbb{F}_q} (2 + \#\pi_{T_a}^{-1}(x)) = 2q + \#T_a.\end{aligned}$$

From Lemma 3, we have $\#T_a = \#\Sigma_a$. Since $\#\mathcal{C}(\mathbb{F}_q) = \#\mathcal{C}_a(\mathbb{F}_q)$, so the proof of this proposition is finished. □

A.2 Cardinality of Σ_a^ϕ

For $a \in \mathbb{F}_q$, let $\mathcal{C}'_a$ be the affine curve that is defined by the equation

$$\mathbf{y}^2 = F_a(\mathbf{x}) = f(a + \mathbf{x}t) f(a - \mathbf{x}t).$$

Remark 4. The affine curve $\mathcal{C}'_a$, for $a \in \mathbb{F}_q$, is defined over $\mathbb{F}_q$ (see [8]). Furthermore,

$$\#\mathcal{C}'_a(\mathbb{F}_q) = \#\{P \in \mathcal{C}(\mathbb{F}_{q^2}) : \ x_P = a + x_1 t, \, x_1 \in \mathbb{F}_q\}.$$

Theorem 3 in [8] gives the bound for $\#\mathcal{C}'_a(\mathbb{F}_q)$.

Proposition 10. *$\#\Sigma_a^\phi = \#\mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q)$, for all $a \in \mathbb{F}_q$.*

Proof. Let $P \in \mathcal{C}(\mathbb{F}_{q^2})$, where $x_P = x_0 + x_1 t$ and $x_0, x_1 \in \mathbb{F}_q$. Since $t^q = -t$, so $x_P + x_{\phi(P)} = 2x_0$. That means $(P, \phi(P)) \in \Sigma_a^\phi$ if and only if $x_0 = \frac{a}{2}$. Then Remark 4 concludes the proof of this proposition. □

A.3 On the Sum of $\#\Sigma_a$ and $\#\Sigma_a^\phi$

In the proof of Theorem 2 (Subsection 4.2), we are dealing to have a tight estimate for $\#\Sigma_a + \#\Sigma_a^\phi$, for all $a \in \mathbb{F}_q$. Following the result of Propositions 9 and 10, one can obtain separate estimates for $\#\Sigma_a$ and $\#\Sigma_a^\phi$. Then add them together to have an estimate for $\#\Sigma_a + \#\Sigma_a^\phi$, for $a \in \mathbb{F}_q$. But this estimate is not tight. Using the result of Proposition 12, we give a tight estimate for it. For the proof of Proposition 12, we need several lemmas.

We recall some details from Subsection 4.2. The two-variable polynomial Φ in $\mathbb{F}_q[\mathbf{x}_0, \mathbf{x}_1]$ is defined as $\Phi(\mathbf{x}_0, \mathbf{x}_1) = f(\mathbf{x}_0) f(\mathbf{x}_1)$. Furthermore, the two-variable polynomial Ψ in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ is defined by

$$\Psi(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^{d} (\mathbf{b} - \lambda_i \mathbf{a} + \lambda_i^2),$$

where λ_i are roots of f in $\overline{\mathbb{F}}_q$. For $a \in \mathbb{F}_q$, the affine curve $\mathcal{X}_a$ is defined over $\mathbb{F}_q$, by the equation

$$\mathbf{y}^2 = \Psi_a(\mathbf{b}) = \Psi(a, \mathbf{b}).$$

Lemma 5. *Define the map $\rho : \mathcal{C}_a^\star(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ by*

$$\rho(x, y) = x(a - x).$$

Let $b \in \mathbb{F}_q$. Assume $\rho^{-1}(b) \neq \emptyset$. Let $(x, y) \in \rho^{-1}(b)$. Then

$$\#\rho^{-1}(b) = \begin{cases} 1, & \text{if } x = \frac{a}{2} \text{ and } y = 0, \\ 2, & \text{if } x = \frac{a}{2} \text{ and } y \neq 0 \text{ or } x \neq \frac{a}{2} \text{ and } y = 0, \\ 4, & \text{otherwise.} \end{cases}$$

Proof. Let $(x, y) \in \rho^{-1}(b)$. It is obvious that $(x, y) \in \rho^{-1}(b)$ if and only if $(x, -y) \in \rho^{-1}(b)$. Furthermore x is a root of polynomial $\tau(\mathbf{x}) = \mathbf{x}^2 - a\mathbf{x} + b$. □

Lemma 6. *Define the map $\varrho : \mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ by*

$$\varrho(x, y) = \frac{a^2}{4} - \alpha x^2.$$

Let $b \in \mathbb{F}_q$. Assume $\varrho^{-1}(b) \neq \emptyset$. Let $(x, y) \in \varrho^{-1}(b)$. Then

$$\#\varrho^{-1}(b) = \begin{cases} 1, & \text{if } x = 0 \text{ and } y = 0, \\ 2, & \text{if } x = 0 \text{ and } y \neq 0 \text{ or } x \neq 0 \text{ and } y = 0, \\ 4, & \text{otherwise.} \end{cases}$$

Proof. Let $(x, y) \in \varrho^{-1}(b)$. It is obvious that $(x, y) \in \varrho^{-1}(b)$ if and only if $(x, -y) \in \varrho^{-1}(b)$. Furthermore x is a root of polynomial $\widetilde{\tau}(\mathbf{x}) = \alpha\mathbf{x}^2 - \frac{a^2}{4} + b$. Thus $(x, y) \in \varrho^{-1}(b)$ if and only if $(-x, y) \in \varrho^{-1}(b)$. □

Lemma 7. *Define the projection map* $\pi : \mathcal{X}_a(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ *by* $\pi(b, y) = b$. *Then*

$$\#\rho^{-1}(b) + \#\varrho^{-1}(b) = 2\#\pi^{-1}(b),$$

for all $b \in \mathbb{F}_q$.

Proof. Let $b \in \mathbb{F}_q$, such that $\pi^{-1}(b) \neq \emptyset$. So there exist a point $(b, y) \in \mathcal{X}_a(\mathbb{F}_q)$. Hence $y^2 = \Psi_a(b) = \Psi(a, b)$. If $y = 0$, then $\pi^{-1}(b) = \{(b, 0)\}$. So $\#\pi^{-1}(b) = 1$. If $y \neq 0$, then $\pi^{-1}(b) = \{(b, y), (b, -y)\}$. Hence $\#\pi^{-1}(b) = 2$. Consider the polynomials $\tau, \widetilde{\tau} \in \mathbb{F}_q[\mathbf{x}]$, that are defined as $\tau(\mathbf{x}) = \mathbf{x}^2 - a\mathbf{x} + b$ and $\widetilde{\tau}(\mathbf{x}) = \alpha\mathbf{x}^2 - \frac{a^2}{4} + b$. Let $\mathcal{D}$ be the discriminant of τ, that is $\mathcal{D} = a^2 - 4b$. Then $\alpha\mathcal{D}$ is the discriminant of $\widetilde{\tau}$. We explain in three cases for $\mathcal{D}$.

First, assume $\mathcal{D} = 0$. Hence $\frac{a}{2}$ is the multiple root of τ. Since $y^2 = \Psi(a, b)$, then $y^2 = \Phi(\frac{a}{2}, \frac{a}{2}) = (f(\frac{a}{2}))^2$. Thus $(\frac{a}{2}, y) \in \mathcal{C}_a^\star(\mathbb{F}_q)$ and $(0, y) \in \mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q)$. Since $\mathcal{D} = 0$, then $b = \frac{a^2}{4}$, so $(\frac{a}{2}, y) \in \rho^{-1}(b)$ and $(0, y) \in \varrho^{-1}(b)$. From Lemmas 5 and 6, if $y = 0$, then $\#\rho^{-1}(b) = \#\varrho^{-1}(b) = 1$, else $\#\rho^{-1}(b) = \#\varrho^{-1}(b) = 2$.

Second, assume $\mathcal{D}$ is a square in $\mathbb{F}_q^*$. So τ is reducible in $\mathbb{F}_q[\mathbf{x}]$. Let x_0, x_1 be the distinct roots of τ in $\mathbb{F}_q$. Then $x_0 + x_1 = a$ and $x_0x_1 = b$. Since $y^2 = \Psi(a, b)$, then $y^2 = \Phi(x_0, x_1) = f(x_0)f(x_1)$. Thus (x_0, y) and (x_1, y) are points of $\mathcal{C}_a^\star(\mathbb{F}_q)$ and $\rho^{-1}(b)$. From Lemma 5, if $y = 0$, then $\#\rho^{-1}(b) = 2$, else $\rho^{-1}(b) = 4$, since x_0 and x_1 do not equal $\frac{a}{2}$. Since $\mathcal{D}$ is a square in $\mathbb{F}_q^*$ and α is a non-square in $\mathbb{F}_q$, then $\alpha\mathcal{D}$, the discriminant of $\widetilde{\tau}$, is a non-square in $\mathbb{F}_q^*$. That means $\widetilde{\tau}(\mathbf{x})$ has no root in $\mathbb{F}_q$. So $\varrho^{-1}(b) = \emptyset$.

Third, assume $\mathcal{D}$ is a non-square in $\mathbb{F}_q$. Hence $\tau(\mathbf{x})$ has no root in $\mathbb{F}_q$. So $\rho^{-1}(b) = \emptyset$. Also $\alpha\mathcal{D}$ is a square in $\mathbb{F}_q^*$. Thus $\widetilde{\tau}$ is reducible in $\mathbb{F}_q[\mathbf{x}]$. Let x_0, x_1 be the distinct roots of $\widetilde{\tau}$ in $\mathbb{F}_q$. Clearly $x_0 = -x_1$ and $x_0x_1 = -\frac{\mathcal{D}}{4\alpha}$. Let $z_0 = \frac{a}{2} + x_0t$ and $z_1 = \frac{a}{2} + x_1t$. Then $z_0 + z_1 = a$ and $z_0z_1 = b$. Since $y^2 = \Psi(a, b)$, then $y^2 = \Phi(z_0, z_1) = f(z_0)f(z_1)$. So $y^2 = F_{\frac{a}{2}}(x_0) = F_{\frac{a}{2}}(x_1)$. Thus (x_0, y) and (x_1, y) are points of $\mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q)$ and $\varrho^{-1}(b)$. From Lemma 6, if $y = 0$, then $\#\varrho^{-1}(b) = 2$, else $\varrho^{-1}(b) = 4$, since x_0 and x_1 do not equal 0.

Now, let $b \in \mathbb{F}_q$, such that $\pi^{-1}(b) = \emptyset$. Then $\rho^{-1}(b) = \varrho^{-1}(b) = \emptyset$. Since if $(x, y) \in \rho^{-1}(b)$, then $x(a - x) = b$ and $(x, y) \in \mathcal{C}_a^\star(\mathbb{F}_q)$. So $y^2 = f(x)f(a - x)$. Then $y^2 = \Phi(x, a - x) = \Psi(a, b) = \Psi_a(b)$. Thus $(b, y) \in \mathcal{X}_a(\mathbb{F}_q)$, which is a contradiction. Also if $(x, y) \in \varrho^{-1}(b)$, then $\frac{a^2}{4} - \alpha x^2 = b$ and $(x, y) \in \mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q)$. Hence $y^2 = f(\frac{a}{2} + xt)f(\frac{a}{2} - xt)$. Then $y^2 = \Phi(\frac{a}{2} + xt, \frac{a}{2} - xt) = \Psi(a, b) = \Psi_a(b)$. Thus $(b, y) \in \mathcal{X}_a(\mathbb{F}_q)$, which is a contradiction. □

Proposition 11. $\#\mathcal{C}_a^\star(\mathbb{F}_q) + \#\mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q) = 2\#\mathcal{X}_a(\mathbb{F}_q)$, *for all* $a \in \mathbb{F}_q$.

Proof. Let $a \in \mathbb{F}_q$. From Lemma 7, $\#\rho^{-1}(b) + \#\varrho^{-1}(b) = 2\#\pi^{-1}(b)$, for all $b \in \mathbb{F}_q$. Then

$$\begin{aligned}\#\mathcal{C}_a^\star(\mathbb{F}_q) + \#\mathcal{C}'_{\frac{a}{2}}(\mathbb{F}_q) &= \sum_{b\in\mathbb{F}_q} \#\rho^{-1}(b) + \sum_{b\in\mathbb{F}_q} \#\varrho^{-1}(b) \\ &= \sum_{b\in\mathbb{F}_q} 2\#\pi^{-1}(b) = 2\#\mathcal{X}_a(\mathbb{F}_q).\end{aligned}$$

□

Proposition 12. *Let $a \in \mathbb{F}_q$. Then*

$$\#\Sigma_a + \#\Sigma_a^\phi = 2(\#\mathcal{C}(\mathbb{F}_q) + \#\mathcal{X}_a(\mathbb{F}_q) - q).$$

Proof. Propositions 9, 10 and 11 conclude the proof of this proposition. □

B Proofs of Propositions

In this section we prove Propositions 4 and 7.

B.1 Proof of Proposition 4

Proof (Proposition 4). Clearly the affine curve $\mathcal{X}_a$ is absolutely irreducible for all $a \in \mathbb{F}_q$. The affine curve $\mathcal{X}_a$ may be singular. Let $\sigma_{i,j} = \lambda_i + \lambda_j$, for all integers i, j such that $1 \leq i < j \leq 5$. Let s_a be the number of $\sigma_{i,j}$ that are equal to a. Then the polynomial $\Psi_a(\mathbf{b})$ has s_a double roots, since λ_i are pairwise distinct. That means $\mathcal{X}_a$ has s_a singular points. Note that $0 \leq s_a \leq 2$. If $s_a = 0$, then $\mathcal{X}_a$ is is an absolutely nonsingular affine curve of genus 2. In fact, the genus of the nonsingular model of $\mathcal{X}_a$ equals $2 - s_a$. By using Hasse-Weil bound for the nonsingular model of $\mathcal{X}_a$, we obtain

$$|\#\mathcal{X}_a(\mathbb{F}_q) - q| \leq 2(2 - s_a)\sqrt{q} + s_a \leq 4\sqrt{q}.$$

So the proof of this proposition is completed. □

B.2 Proof of Proposition 7

Proof (Proposition 7). Let $b \in \mathbb{F}_q$. Let $\delta_{i,j} = \lambda_i\lambda_j$, for all integers i, j such that $1 \leq i < j \leq 5$. Let s_b be the number of $\delta_{i,j}$ that are equal to b. Then the polynomial $\Psi_b(\mathbf{a})$ has s_b double roots, since λ_i are pairwise distinct.

If $f(0) \neq 0$, then $\lambda_i \neq 0$, for all integer $0 \leq i \leq 5$. Then the degree of $\Psi_b(\mathbf{a})$ equals 5. So the affine curve $\mathcal{X}_b$ is absolutely irreducible for all $b \in \mathbb{F}_q$. Since $\Psi_b(\mathbf{a})$ has s_b double root, thus $\mathcal{X}_b$ has s_b singular points. In fact, the genus of the nonsingular model of $\mathcal{X}_b$ equals $2 - s_b$. By using Hasse-Weil bound for the the number of $\mathbb{F}_q$-rational points of the nonsingular model of $\mathcal{X}_b$, we obtain

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq 2(2 - s_b)\sqrt{q} + s_b \leq 4\sqrt{q}.$$

If $f(0) = 0$, then there exists an integer i such that $\lambda_i = 0$. If $b = 0$, clearly $\#\mathcal{X}_b(\mathbb{F}_q) = q$. Now assume that $b \neq 0$. Then the degree of $\Psi_b(\mathbf{a})$ equals 4. In this case, one could show that, $s_b = 2$ if and only if $b \in I_f$. If $s_b = 2$, then $\Psi_b(\mathbf{a})$ is square, so the affine curve $\mathcal{X}_b$ is reducible. Hence we have only the trivial bound for $\#\mathcal{X}_b(\mathbb{F}_q)$, that is

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq q.$$

Otherwise $s_b \leq 1$. So $\Psi_b(\mathbf{a})$ is a non-square. Hence the affine curve $\mathcal{X}_b$ is absolutely irreducible. Furthermore $\mathcal{X}_b$ has s_b singular points and the genus of the nonsingular model of $\mathcal{X}_b$ equals $1 - s_b$. By using Hasse-Weil bound we obtain

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq 2(1 - s_b)\sqrt{q} + s_b \leq 2\sqrt{q}.$$

So the proof of this proposition is finished. □